Major problem for an enterprise: «How to know if I am compliant with the GDPR (and not be fined)?»

Can these (partially) bridge the gap to achieve GDPR compliance?

Are there any possible matchings? Such as...

**GDPR**
- Data minimization (art. 5)
- Data categories (art. 9)
- Appropriate measures (art. 30)
- Risk assessment (art. 33)
- Data protection officer (art. 35)
- Data transfer (art. 41)

**ISO 27001:2013**
- Information security risk assessment (art. 8.2.1)
- Management responsibilities (A.7.2.1)
- Classification of information (A.8.2.1)
- Management of access rights (A.9.2.3)
- Information transfer policies (A.13.2.1)
- Information security (A.14.1)

Benefits for many stakeholders
- Security standards as "partial" data protection standards
- Less changes needed to achieve compliance
- Easier to define actual standards for data protection
- Faster adaptation
- Less likely to incur into penalties

Endorsed by the Luxembourg Privacy Cluster (LPC)
University of Luxembourg

This work is within the scope of a joint work at SnT (Interdisciplinary Centre for Security, Reliability and Trust) within the scope of the data protection reform in cloud systems
E-mail contact of the authors: {firstname.lastname}@uni.lu